STAT

ARTICLE APPEARED ON PAGE 4-A

WASHINGTON TIMES
30 March 1987

Reagan crackdown stirs debate over fighting Soviet espionage

By Bill Gertz
THE WASHINGTON TIMES

Beginning in the late 1970s, Western intelligence officials started receiving thousands of documents on Soviet technological espionage turned over by a secret agent inside the Soviet military-industrial complex.

According to intelligence officials, the documents were sobering: They revealed a massive Soviet weapons-building program based in part on technology the Soviets planned to steal or purchase, often illegally, from advanced Western nations.

To counter the effort, the Reagan administration in 1981 launched a major strategic program to block the acquisition of Western know-how and hardware destined for Soviet military systems.

The policy has led to debate among security experts and information specialists over the government's efforts to ferret out Soviet electronic spies from government and private telecommunications systems, considered a major source of defense- and weapons-related information.

At the center of the controversy is a 1984 adminstration policy directive know as National Security Decision Directive 145, which established an inter-agency group of U.S. officials to deal with the problem.

In only one of several anti-spying successes stemming from the directive, the National Security Agency uncovered a Soviet high-tech espionage program at the U.S. embassy in Moscow, intelligence sources said.

NSA, during a search of the embassy, discovered that the Soviets had planted electronic listening devices inside U.S. typewriters and were able to read secret U.S. communications between 1985 and 1986, sources said.

Yet despite the successes, the National Security Council, under pressure from a House subcommittee headed by Rep. Jack Brooks, Texas Democrat, two weeks ago lifted a directive issued by the inter-agency group last May. The NSC also is reviewing the entire policy in what some security officials consider a retreat from earlier policies.

The directive broadly defined the scope of technical information available to the public that could be pieced together in a "mosaic" by the Soviets to obtain secret national security information.

Critics, led by Mr. Brooks and the computer services industry, charge the administration is attempting to inhibit the free flow of electronic information by intruding upon the private sector in its search for Soviet electronic spies.

Kenneth de Graffenreid, a former White House intelligence official and a leading supporter of a tough anti-electronic espionage measures, believes the computer security policy is appropriate and necessary. Two weeks ago he testified before the Brooks subcommittee that the Soviets have been operating a "massive and highly sophisticated" electronic spy program.

Critics ... charge the administration is attempting to inhibit the free flow of information in its search for Soviet electronic spies.

"I was eager to defend 145 because it's an eminently defensible position," Mr. de Graffenreid said in a recent interview. "There appears to be some retreat from it, but it's the flagship of our efforts."

Mr. de Graffenreid said the critics' perception of the policy is different from the reality. The program is aimed solely at protecting equipment, not information, from unauthorized use, he said.

Angelo Codevilla, an intelligence expert with the Hoover Institution in Stanford, Calif., said the problem of information security has been compounded by recent administration actions to declassify volumes of information once regarded as secret.

"But if more is to be declassified, then much more responsibility needs to be exercised about how sensitive, unclassified information is used," Mr. Codevilla said in an interview.

Until last year, Mr. Codevilla worked with the administration in helping to formulate the policy directives as a Senate Intelligence Committee staff member and aide to Sen. Malcolm Wallop, Wyoming Republican.

"The program was designed literally as a public service to help private individuals make intelligent choices about how they would handle this information," he said. Without the help, "they would be flying blind."

Soviet electronic spying poses a serious threat and "communications are being intercepted every day," Mr. Codevilla said.

"The U.S. government, if it cannot stop the Soviets from doing it, at least owes it to the American people to let us know what the Soviets are intercepting," he said.

An administration intelligence official was more blunt about the recent NSC changes. "There was no reason to revoke that stuff," the source said. "It was no grand threat to civil liberties."

The official, who declined to be named, said the security policy was intitiated as an attempt to centralize authority within the Defense Department, rather than have separate agencies approach the problem in different ways.

"NSA, under the guidelines, has no capability to demand anything," the official said. "But they can provide services in economically reasonsable ways. If material is being stolen, a company should be told about it — the government has an obligation to tell people about when something harms the national security."

Under the administration policy, none of the private sector information service companies are mandated to comply with any of the U.S. government programs, the official said.

Jerry Young, corporate counsel

for Mead Data Central, an Ohio computer service that provides its clients with a data base of published news and trade publications, said his company was contacted by U.S. investigators last April.

"Basically they were responding to N.S.D.D. 145 and a government white paper of September 1985 relating to the Soviet acquisition of militarily significant technology," Mr. Young said in an interview. "They asked us whether we would be willing to block access to the database to certain customers and we said we would not. It's all public information, and we feel it should not be subject to classification."

Mr. Young said the group identified itself as the Air Force Assistance Management Group.

"Then they asked us if we would turn over the names of customers and we said absolutely not," Mr Young said. "We felt very strongly that this was confidential and that we would go to great lengths to keep it that way."

A short time after the visit, the company cancelled its subscription to the Commerce Department's National Technical Information Service, which has been a major target of Soviet information collection efforts. Mr. Young said the step was primarily an "economic decision."

"However, we also felt that without NTIS there was absolutely no justifiation for their concern about people gaining access to our database," he said. "We wanted to draw the line so it was absolutely clear."

Jerry Berman, an American Civil Liberties Union attorney involved in national security issues, said the computer security program poses a threat to constitutional safeguards on the free flow of information. Visits by government agents to private computer firms could have a chilling effect, he said.

"We think the lifting of the policy, because it was so broad, is a step in the right direction," said Mr. Berman. "We are anxious for the government to clarify that its function is to protect systems from unauthorized penetration from outsiders and not for the government to be defining information."

Mr. Berman said he believes the Defense Department and its electronic intelligence component, the National Security Agency, are not the best federal agencies to control the program because they are overly concerned with secrecy.